

Notice of Allowability

Application No.

10/658,340

Examiner

Thomas R. Peeso

Applicant(s)

FUJISAKI ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to application papers filed.
2. ☒ The allowed claim(s) is/are 1-10.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some* c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 10Sep2003
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

THOMAS R. PEESO
PRIMARY EXAMINER

REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance: Applicant has claimed uniquely distinct features in the instant invention which are not found in the prior art, either singularly or in combination. According to an aspect related to the present invention, an encryption apparatus includes an encryption operation unit configured to perform a non-linear function, said encryption operation unit being provided with a Feistel type encryption algorithm and configured to output encrypted data; and a changing unit configured to change a result of an encryption operation into irrelevant data for output to the non-linear function, wherein said changing unit starts changing the result into said irrelevant data after said encrypted data is output. According to another aspect related to the present invention, An encryption apparatus includes an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including: a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to output the non-linearly transformed result value, a logical operation circuit configured to logically operate on the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and a changing module configured to change said key information input into said non-linear transformation circuit into a value unrelated to said key information, wherein said changing module begins execution after said

encrypted data is output from said encryption processing unit. According to another aspect related to the present invention, an encryption apparatus includes an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including: a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to output the non-linearly transformed result value, a logical operation circuit configured to logically operate the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and a first changing unit configured to change said first data. According to another aspect related to the present invention, An encryption apparatus includes an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including: a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to output the non-linearly transformed result value, a logical operation circuit configured to logically operate on the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and a changing

module configured to change said key information input into said non-linear transformation circuit into a value unrelated to said key information, wherein said changing module begins execution after said encrypted data is output from said encryption processing unit. According to another aspect related to the present invention, an encryption apparatus includes an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including: a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to output the non-linearly transformed result value, a logical operation circuit configured to logically operate the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and a first changing unit configured to change said first data

3

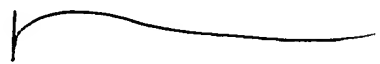
These features are not found or suggested in the prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas R. Peeso whose telephone number is 571 272-3809. The examiner can normally be reached on Mon.-Fri, 7:00 a.m. to 3:30 p.m. The central fax number for the office is 571 273-8300.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571 272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Thomas R. Peeso
Primary Examiner

26 September 2006